REMARKS

Applicant would like to thank the Examiner for the thorough examination of the present application. The arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in independent Claim 1, for example, is directed to a block cipher device for a cryptographically secured digital communication system comprising a pair of first stages connected in parallel and receiving an input data block and a control data block. Each first stage defines a respective first data path and comprises a sum modulo-two unit responsive to the control data block and the input data block, and a first nibble swap unit is downstream from the sum modulo-two unit and is responsive to an output signal therefrom and the control data block for reordering the output signal from the sum modulo-two unit.

A diffuser is connected in both of the first data paths for mixing data therebetween. A key scheduler receives a key data block and generates a random key data block based thereon. A pair of second stages is connected in parallel downstream from the first stages and receives the random key data block, the control data block and output signals from the first stages. Each second stage defines a respective second data path and comprises a first linear modulo unit responsive to the random key data block, one of the output signals from the first stages, and the control data block for performing a modulo summing operation based on a first modulus q. An n^{th} power modulo unit is

responsive to an output signal from the first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p. A second linear modulo unit is responsive to the random key data block and an output signal from the n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r. Each first, second and third modulus q, p and r is unique from each other. An output stage is connected to the second stages for generating an output data block for the block cipher device.

The claimed invention advantageously provides a more secure cryptography system that is also compatible with existing less secure cryptography systems. Since there are two data paths in the block cipher device, a larger number of bits can be accommodated since the size of the input data block and the size of the key data block may be increased. Supporting a larger number of bits increases the cryptographic strength of the block cipher device.

Another advantageous feature of the block cipher device is that it is backward compatible with cryptography systems that are less secure, i.e., those operating with smaller size input data blocks and smaller size key data blocks. Backward compatibility may be accomplished by providing the smaller size input data block to one of the respective first and second data paths in the first and second stages, and by bypassing the bit diffuser. Likewise, the key scheduler may generate a random key data block for the data path that is operational.

Independent Claim 13 is directed to a communication system comprising the block cipher device for converting an input

data block into an output data block, and is similar to independent Claim 1.

Independent Claim 29 is directed to a method for converting an input data block into an output data block for a cryptographically secured digital communication system, and is similar to independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 13 and 29 over the Kurdziel et al. patent in view of the Rogaway published patent application. The Examiner cited Kurdziel et al. as disclosing the claimed invention except for a diffuser connected in both of the first data paths for mixing data therebetween. The Examiner cited Rogaway as disclosing the diffuser.

As best illustrated in FIG. 4 of Kurdziel et al., the illustrated block cipher device **100** includes a first stage for receiving an input data block **X** and a control data block $\mathbf{Z_1}$. The first stage defines a first data path, and includes a sum modulo-two unit **1** and a first nibble swap unit **2** downstream from the sum modulo-two unit.

A key scheduler **9** receives a key data block $\mathbf{Z_6}$ and generates a random key data block $\mathbf{Z_7}$ based thereon. A second stage is connected downstream from the first stage and receives the random key data block $\mathbf{Z_7}$, the control data block $\mathbf{Z_5}$ and output signals from the first stage. Each second stage defines a second data path, and includes a first linear modulo unit **5** and an n^{th} power modulo unit **6** downstream from the first linear modulo unit.

An output stage **11** is connected to the second stages for generating an output data block for the block cipher device.

The Examiner has characterized the first stage in Kurdziel et al. as including a pair of first stages connected in parallel, and the second stage in Kurdziel et al. as including a pair of second stages connected in parallel. The Applicant submits that the Examiner has simply mischaracterized Kurdziel et al. in terms of providing parallel data paths. The Examiner seems to support his characterization of parallel data paths based on column 2, lines 10-13 of Kurdziel et al., which provides:

> "The structure of the input unit **10** and output unit **11** generally depends on an application (e.g., serial or parallel)." (Emphasis added).

It appears that the Examiner has interpreted this to mean that for a "parallel" application, a pair of first stages must be connected in parallel, with each first stage defining a respective first data path. The same interpretation may be applied to the second stage.

Please note that the Applicant is also an inventor in Kurdziel et al., and the Applicant respectfully submits that the Examiner has erroneously interpreted column 2, lines 10-13 in Kurdziel et al. The "serial or parallel" application in column 2, lines 10-13 simply refers to whether a host equipment is interfacing the block cipher device **100** via a bus (parallel) or via a serial bit stream. The input and output units **10, 11** format

the data coming in from the host equipment into data blocks for processing by the block cipher device **100**. For example, if the host equipment provides data via a serial bit stream, the input unit **10** will perform a serial to parallel data conversion. Alternatively, if the data came via a parallel bus, then the input unit **10** would simply accumulate the bus-width packets until a full block was obtained. The same holds true for the output block **11**, but only in reverse.

The Examiner appears to have interpreted the above-referenced "serial or parallel" reference as if, depending on the application, you would deploy parallel renderings of the algorithm. This is not correct. The structure of the cryptographic algorithm in Kurdziel et al. conforms to the disclosed theoretical foundation - which operates on a single data path in the first and second stages.

In sharp contrast, the Applicant recognized the shortfalls of his cited prior art reference, and improved upon it in the present invention. The subject of the present invention conforms to this foundation by operating on parallel data paths in the first and second stages. The Applicant submits that the design required much more acumen than simply running two processes in parallel with a mixer or diffuser cross linking them. Such an approach like that would have provided a design with inferior cryptographic strength.

As a result of the first and second parallel data paths, the claimed invention advantageously provides a more secure cryptography system that is also compatible with existing

less secure cryptography systems. Since there are two data paths in the block cipher device, a larger number of bits can be accommodated since the size of the input data block and the size of the key data block may be increased. Supporting a larger number of bits increases the cryptographic strength of the block cipher device.

Another advantageous feature of the block cipher device is that it is backward compatible with cryptography systems that are less secure, i.e., those operating with smaller size input data blocks and smaller size key data blocks. Backward compatibility may be accomplished by providing the smaller size input data block to one of the respective first and second data paths in the first and second stages, and by bypassing the bit diffuser. Likewise, the key scheduler may generate a random key data block for the data path that is operational.

Referring now to Rogaway, the Examiner cited this reference as disclosing a diffuser connected in the first data path for mixing data. Rogaway discloses a wide-block size block cipher that takes a possibly long string as plaintext and turns it into a cipher text having the same length as the plaintext. The wide-block size block cipher is made from a conventional block cipher, which is a block cipher that operates on strings of some small, fixed length. The wide-block size block cipher is obtained from the conventional block cipher by a three-step process. The first step is to encipher the plaintext using some mode of operation of the conventional block cipher. The second step is to mask the resulting intermediate value by way of a computationally cheap mixing step. The third step is to decipher

the masked intermediate value using some mode of operation of the conventional block cipher. The Examiner characterized the mixing step as the diffuser.

Even if the references were selectively combined as suggested by the Examiner, the claimed invention is still not provided. Kurdziel et al. only discloses a single data path in the first and second stages, and Rogaway fails to provide this noted deficiency.

Accordingly, it is submitted that independent Claim 1 is patentable over Kurdziel et al. in view of Rogaway. Independent Claims 13 and 29 are similar to independent Claim 1. Therefore, it is submitted that these claims are also patentable over Kurdziel et al. in view of Rogaway. In view of the patentability of the independent Claims 1, 13 and 29, it is submitted that their dependent claims, which recite yet further distinguishing features of the invention, are also patentable. These dependent claims require no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**

_____/

Michael W. Taylor

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330